



# FortiManager - Release Notes

Version 6.4.7

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



November 30, 2022

FortiManager 6.4.7 Release Notes

02-647-739263-20221130

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>FortiManager 6.4.7 Release</b>	<b>7</b>
Supported models	7
FortiManager VM subscription license	7
Management extension applications	8
Supported models for MEA	8
Minimum system requirements	8
<b>Special Notices</b>	<b>9</b>
View Mode is disabled in policies when policy blocks are used	9
Custom signature filenames	9
SDN fabric connectors	9
ADOM version enforcement	9
Management Extension Applications (MEA) and upgrade	10
Policy Hit Count on unused policy	10
Wireless Manager (FortiWLM) not accessible	10
SD-WAN Orchestrator not accessible	10
Support for FortiOS 6.4 SD-WAN Zones	10
FortiGuard Rating Services with FortiGate 6.4.1 or Later	11
Citrix XenServer default limits and upgrade	11
Multi-step firmware upgrades	11
Hyper-V FortiManager-VM running on an AMD CPU	11
SSLv3 on FortiManager-VM64-AWS	12
<b>Upgrade Information</b>	<b>13</b>
Downgrading to previous firmware versions	13
Firmware image checksums	13
FortiManager VM firmware	13
SNMP MIB files	15
<b>Product Integration and Support</b>	<b>16</b>
FortiManager 6.4.7 support	16
Web browsers	17
FortiOS/FortiOS Carrier	17
FortiADC	17
FortiAnalyzer	17
FortiAuthenticator	17
FortiCache	17
FortiClient	18
FortiDDoS	18
FortiMail	18
FortiSandbox	18
FortiSOAR	19
FortiSwitch ATCA	19
FortiTester	19

FortiWeb .....	19
Virtualization .....	20
Feature support .....	20
Language support .....	21
Supported models .....	21
FortiGate models .....	22
FortiGate special branch models .....	24
FortiCarrier models .....	25
FortiADC models .....	26
FortiAnalyzer models .....	26
FortiAuthenticator models .....	28
FortiCache models .....	28
FortiDDoS models .....	28
FortiMail models .....	29
FortiProxy models .....	29
FortiSandbox models .....	29
FortiSOAR models .....	30
FortiSwitch ATCA models .....	30
FortiTester models .....	30
FortiWeb models .....	31
<b>Compatibility with FortiOS Versions .....</b>	<b>33</b>
FortiManager 6.4.7 and FortiOS 6.4.9 compatibility issues .....	33
<b>Resolved Issues .....</b>	<b>35</b>
AP Manager .....	35
Device Manager .....	35
FortiSwitch Manager .....	37
Global ADOM .....	37
Others .....	37
Policy and Objects .....	38
Revision History .....	40
Script .....	40
Services .....	41
System Settings .....	41
VPN Manager .....	42
<b>Known Issues .....</b>	<b>43</b>
Device Manager .....	43
Others .....	43
Policy & Objects .....	43
Revision History .....	44
Script .....	44
Services .....	44
System Settings .....	44
<b>Appendix A - FortiGuard Distribution Servers (FDS) .....</b>	<b>45</b>
FortiGuard Center update support .....	45

---

<b>Appendix B - Default and maximum number of ADOMs supported .....</b>	<b>46</b>
Hardware models .....	46
Virtual Machines .....	46

# Change Log

Date	Change Description
2021-09-02	Initial release.
2021-09-07	Updated <a href="#">Appendix B - Default and maximum number of ADOMs supported on page 46</a> . Added <a href="#">FortiTester models on page 30</a> .
2021-09-10	Added FortiGate-1801F to <a href="#">FortiGate models on page 22</a> .
2021-09-27	Removed FortiSandbox 4.0.
2021-09-28	Moved FortiGate-1801F from FortiGate models to <a href="#">FortiGate special branch models on page 24</a> .
2021-10-05	Removed 604125, 692669, 667197 from <a href="#">Known Issues on page 43</a> .
2021-10-18	Updated 704637 in <a href="#">Resolved Issues on page 35</a> .
2021-11-22	Added FMG-400G to <a href="#">Supported models on page 7</a> .
2021-11-26	Added Microsoft Hyper-V Server 2019 to <a href="#">Virtualization on page 20</a> and removed 695782 from <a href="#">Resolved Issues on page 35</a> .
2021-12-10	Updated <a href="#">FortiOS/FortiOS Carrier on page 17</a> .
2021-12-15	Updated <a href="#">FortiMail models on page 29</a> .
2021-12-21	Updated FortiWiFi models in <a href="#">FortiGate models on page 22</a> .
2022-01-06	Updated <a href="#">FortiGate models on page 22</a> .
2022-01-24	Updated <a href="#">FortiGate models on page 22</a> to show 6.2 and 6.0 support for FortiGate-3600E and FortiGate-3601E. Updated <a href="#">FortiSandbox models on page 29</a> to include FSA-3000F.
2022-02-08	Added FMG-3700G to <a href="#">Supported models on page 7</a> .
2022-02-23	Added special notice to <a href="#">Special Notices on page 9</a> .
2022-03-02	Updated <a href="#">Special Notices on page 9</a> .
2022-03-23	Updated <a href="#">FortiGate models on page 22</a> .
2022-04-07	Updated <a href="#">Special Notices on page 9</a> .
2022-05-02	Added support for FortiOS 6.4.9 to <a href="#">FortiOS/FortiOS Carrier on page 17</a> .
2022-07-18	Added <a href="#">FortiManager 6.4.7 and FortiOS 6.4.9 compatibility issues on page 33</a> .
2022-10-20	Added 765709 to <a href="#">Known Issues on page 43</a> and updated <a href="#">FortiManager 6.4.7 and FortiOS 6.4.9 compatibility issues on page 33</a> .
2022-11-30	Updated <a href="#">FortiGate models on page 22</a> .

# FortiManager 6.4.7 Release

This document provides information about FortiManager version 6.4.7 build 2412.



The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 7](#)
- [FortiManager VM subscription license on page 7](#)
- [Management extension applications on page 8](#)

## Supported models

FortiManager version 6.4.7 supports the following models:

<b>FortiManager</b>	FMG-200F, FMG-200G, FMG-300E, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, FMG-3900E, and FMG-4000E.
<b>FortiManager VM</b>	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

## FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see [FortiManager VM firmware on page 13](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 46](#).



You can use the FortiManager VM subscription license with new FMG-VM installations. For existing FMG-VM installations, you cannot upgrade to a FortiManager VM subscription license. Instead, you must migrate data from the existing FMG-VM to a new FMG-VM with subscription license.

## Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 6.4.7.



FortiManager uses port TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the [FortiManager 6.4 Ports and Protocols Guide](#).

## Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

<b>FortiManager</b>	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3700G, FMG-3900E, and FMG-4000E.
<b>FortiManager VM</b>	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

## Minimum system requirements

Some management extension applications supported by FortiManager 6.4.7 have minimum system requirements. See the following table:

Management Extension Application	Minimum system requirement
<b>SD-WAN Orchestrator</b>	At least 12GB of memory is recommended to support SD-WAN Orchestrator MEA.
<b>Wireless Manager (WLM)</b>	A minimum of 4 CPU cores and 8 GB RAM is typically required. Depending on the number of running applications, the allocated resources should be increased.



# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.4.7.

## View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain multiple policies using different incoming and outgoing interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

## Custom signature filenames

Custom signature filenames are limited to a maximum of 50 characters because FortiManager appends the VDOM suffix to custom signature filenames when FortiGate uses VDOMs.

## SDN fabric connectors

According to the current design, SDN fabric connectors are installed on all FortiGates in an ADOM, even if the fabric connectors are not in use. See also bug ID 496870 in [Known Issues on page 43](#).

**Workaround:** Place FortiGates in another ADOM when you do not want to install SDN fabric connectors to the devices.

## ADOM version enforcement

Starting in FortiManager 6.4.6, ADOM versions are enforced. ADOM version N and N+1 are allowed, and the enforcement affects policy package installation.

For example, if you have ADOM version 6.0, and it contains a FortiGate running FortiOS 6.4, you cannot install a version 6.0 policy package to the FortiGate. The policy package installation fails with the following error message: `Device preparation failed: version mismatched, adom:6.0; dev:6.4.`

## Management Extension Applications (MEA) and upgrade

Upgrading FortiManager when Management Extension Applications (MEA) are enabled may reset your *System Settings* to the default settings.

To prevent your *System Settings* from being lost, please disable all Management Extension Applications (MEA) prior to upgrading FortiManager.

## Policy Hit Count on unused policy

FortiManager 6.4.3 and later no longer displays policy hit count information on the *Policy & Objects > Policy Packages* pane. However, you can view hit count information by using the *Unused Policies* feature and clearing the *Unused Only* checkbox. For more information, see the [FortiManager 6.4 New Features Guide](#).

## Wireless Manager (FortiWLM) not accessible

If Wireless Manager was enabled in FortiManager 6.4.0, you can no longer access it in the FortiManager GUI when you upgrade FortiManager to 6.4.2. When you try to access FortiWLM, you are redirected to the FortiManager dashboard.

## SD-WAN Orchestrator not accessible

If SD-WAN Orchestrator was enabled in FortiManager 6.4.1, you can no longer access it in the FortiManager GUI after upgrading to FortiManager 6.4.2.

To workaround this issue, run the following CLI command to manually trigger an update of SD-WAN Orchestrator to 6.4.1 r2:

```
diagnose docker upgrade sdwancontroller
```

## Support for FortiOS 6.4 SD-WAN Zones

In 6.4 ADOMs, SD-WAN member interfaces are grouped into SD-WAN zones. These zones can be imported as normalized interfaces and used in firewall policies.



Customers upgrading FortiGates from FortiOS 6.2 to 6.4 who cannot upgrade the ADOM are advised to temporarily disable SD-WAN central management until they can upgrade the ADOM to 6.4. This is to prevent FortiManager from attempting to delete the newly created SD-WAN zones on the FortiGate.

---

## FortiGuard Rating Services with FortiGate 6.4.1 or Later

FortiManager 6.4.1 or later is the supported version to provide FortiGuard rating services to FortiGate 6.4.1 or later.

## Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

### To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:

```
xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
```

2. Confirm the setting is in effect by running `xenstore-ls`.

```
-----  
limits = ""  
pv-kernel-max-size = "33554432"  
pv-ramdisk-max-size = "536,870,912"  
boot-time = ""  
-----
```

3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

---

## Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

## Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

## SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol tlsv1
end
```

# Upgrade Information

You can upgrade FortiManager 6.2.0 or later directly to 6.4.7.



For other upgrade paths and details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

---

This section contains the following topics:

- [Downgrading to previous firmware versions on page 13](#)
- [Firmware image checksums on page 13](#)
- [FortiManager VM firmware on page 13](#)
- [SNMP MIB files on page 15](#)

## Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. In addition the local password is erased.

A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}  
execute format {disk | disk-ext4 | disk-ext3}
```

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

## FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

## Aliyun

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

## Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

## Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

## Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

## Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

## Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

---

## VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the [FortiManager Data Sheet](#) available on the Fortinet web site. VM installation guides are available in the [Fortinet Document Library](#).

---

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

# Product Integration and Support

This section lists FortiManager 6.4.7 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [FortiManager 6.4.7 support on page 16](#)
- [Feature support on page 20](#)
- [Language support on page 21](#)
- [Supported models on page 21](#)

## FortiManager 6.4.7 support

This section identifies FortiManager 6.4.7 product integration and support information:

- [Web browsers on page 17](#)
- [FortiOS/FortiOS Carrier on page 17](#)
- [FortiADC on page 17](#)
- [FortiAnalyzer on page 17](#)
- [FortiAuthenticator on page 17](#)
- [FortiCache on page 17](#)
- [FortiClient on page 18](#)
- [FortiDDoS on page 18](#)
- [FortiMail on page 18](#)
- [FortiSandbox on page 18](#)
- [FortiSOAR on page 19](#)
- [FortiSwitch ATCA on page 19](#)
- [FortiTester on page 19](#)
- [FortiWeb on page 19](#)
- [Virtualization on page 20](#)



To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```



Always review the Release Notes of the supported platform firmware version before upgrading your device.

---



## Web browsers

This section lists FortiManager 6.4.7 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 91
- Google Chrome version 92

Other web browsers may function correctly, but are not supported by Fortinet.

## FortiOS/FortiOS Carrier

This section lists FortiManager 6.4.7 product integration and support for FortiOS/FortiOS Carrier:

- 6.4.0 to 6.4.9
- 6.2.0 to 6.2.10
- 6.0.0 to 6.0.14

## FortiADC

This section lists FortiManager 6.4.7 product integration and support for FortiADC:

- 6.0.1
- 5.4.4

## FortiAnalyzer

This section lists FortiManager 6.4.7 product integration and support for FortiAnalyzer:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

## FortiAuthenticator

This section lists FortiManager 6.4.7 product integration and support for FortiAuthenticator:

- 6.0. to 6.3
- 5.0 to 5.5
- 4.3

## FortiCache

This section lists FortiManager 6.4.7 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

## FortiClient

This section lists FortiManager 6.4.7 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.1 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

## FortiDDoS

This section lists FortiManager 6.4.7 product integration and support for FortiDDoS:

- 5.4.2
- 5.3.1
- 5.2.0
- 5.1.0
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see [Feature support on page 20](#).

## FortiMail

This section lists FortiManager 6.4.7 product integration and support for FortiMail:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.10 and later
- 5.4.12
- 5.3.13

## FortiSandbox

This section lists FortiManager 6.4.7 product integration and support for FortiSandbox:

- 4.0.2
- 3.2.2
- 3.1.4
- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

## FortiSOAR

This section lists FortiManager 6.4.7 product integration and support for FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

## FortiSwitch ATCA

This section lists FortiManager 6.4.7 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

## FortiTester

This section lists FortiManager 6.4.7 product integration and support for FortiTester:

- 3.9
- 3.8
- 3.7

## FortiWeb

This section lists FortiManager 6.4.7 product integration and support for FortiWeb:

- 6.3.15
- 6.2.5
- 6.1.2
- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

## Virtualization

This section lists FortiManager 6.4.7 product integration and support for virtualization:

- Amazon Web Services (AWS)
- Citrix XenServer 6.0+ and Open Source Xen 4.1+
- Linux KVM
- Microsoft Azure
- Microsoft Hyper-V 2008 R2, 2012, 2012 R2, 2016, and 2019
- VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7, and 7.0
- Nutanix AHV (AOS 5.10.5)
- Google Cloud (GCP)
- Oracle Cloud Infrastructure (OCI)
- Alibaba Cloud (AliCloud)

## Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC		✓		
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSOAR		✓		
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

## Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiAnalyzer Administration Guide*.

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.4.7.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

- [FortiGate models on page 22](#)
- [FortiGate special branch models on page 24](#)
- [FortiCarrier models on page 25](#)
- [FortiADC models on page 26](#)
- [FortiAnalyzer models on page 26](#)
- [FortiAuthenticator models on page 28](#)
- [FortiCache models on page 28](#)
- [FortiDDoS models on page 28](#)

- [FortiMail models on page 29](#)
- [FortiProxy models on page 29](#)
- [FortiSandbox models on page 29](#)
- [FortiSOAR models on page 30](#)
- [FortiSwitch ATCA models on page 30](#)
- [FortiTester models on page 30](#)
- [FortiWeb models on page 31](#)

## FortiGate models

Model	Firmware Version
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <b>FortiGate 6000 Series:</b> FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC <b>FortiGate 7000 Series:</b> FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F <b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC <b>FortiGate Hardware Low Encryption:</b> FortiGate-100D-LENC <b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F <b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM <b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen <b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4

Model	Firmware Version
<b>FortiGate:</b> FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-60F, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-100F, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1100E, FortiGate-1101E, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <b>FortiGate 6000 Series:</b> FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC <b>FortiGate 7000 Series:</b> FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F <b>FortiGate DC:</b> FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC <b>FortiGate Hardware Low Encryption:</b> FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC <b>FortiWiFi:</b> FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F, FortiWiFi-80F-2R, FortiWiFi-81F-2R, FortiWiFi-81F-2R-3G4G-POE, FortiWiFi-81F-2R-POE <b>FortiGate-VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager <b>FortiGate Rugged:</b> FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G <b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.2

Model	Firmware Version
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FortiGate-60F, FortiGate-61F, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FortiGate-100F, FortiGate-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FortiGate-2200E, FortiGate-2201E, FG-2500E, FortiGate-3300E, FortiGate-3301E, FG-3000D, FG-3100D, FG-3200D, FortiGate-3600E, FortiGate-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E <b>FortiGate 5000 Series:</b> FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate 6000 Series:</b> FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC <b>FortiGate 7000 Series:</b> FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F <b>FortiGate DC:</b> FG-401E-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3600E-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC <b>FortiGate Hardware Low Encryption:</b> FG-100D-LENC, FG-600C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-40F, FWF-40F-3G4G, FWF-41F, FWF-41F-3G4G, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0

## FortiGate special branch models

The following FortiGate models are released on a special branch of FortiOS. FortiManager supports these models.

Model	Firmware Version
<b>FortiGate:</b> FortiGate-200F, FortiGate-201F, FortiGate-1800F, FortiGate-1801F, FortiGate-2600F, FortiGate-2601F, FortiGate-3500F, FortiGate-3501F, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F <b>FortiGate DC:</b> FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC	6.4



Model	Firmware Version
<b>FortiGate:</b> FortiGate-30E-3G4G-GBL, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-200F, FortiGate-201F, FortiGate-1800F, FortiGate-1801F, FortiGate-2600F, FortiGate-2601F, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F <b>FortiGate DC:</b> FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, 4400F-DC, FortiGate-4401F-DC <b>FortiGate Rugged:</b> FortiGateRugged-90D <b>FortiWiFi:</b> FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ,	6.2
<b>FortiGate:</b> FortiGate-30E-3G4G-GBL, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-600E, FortiGate-601E, FortiGate-1800F, FortiGate-1801F, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E <b>FortiGate DC:</b> FortiGate-1100E-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-3400E-DC, FortiGate-3401E-DC <b>FortiGate VM:</b> FortiGate-VM64-RAXONDEMAND <b>FortiWiFi:</b> FortiWiFi-41F, FortiWiFi-41F-3G4G,	6.0

## FortiCarrier models

Model	Firmware Version
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier 6000 Series:</b> FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC <b>FortiCarrier 7000 Series:</b> FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier 6000 Series:</b> FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC	6.2

Model	Firmware Version
<b>FortiCarrier 7000 Series:</b> FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E <b>FortiCarrier 6000 Series:</b> FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC <b>FortiCarrier 7000 Series:</b> FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC <b>FortiCarrier-VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0

## FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

## FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E	6.4

Model	Firmware Version
<b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	
<b>FortiAnalyzer:</b> FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E.	6.2
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.	6.0
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.	5.6
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.	5.4
<b>FortiAnalyzer VM:</b> FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B	5.2
<b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B	5.0
<b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	

## FortiAuthenticator models

Model	Firmware Version
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	6.0 to 6.3
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	5.0 to 5.5
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	4.3

## FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E <b>FortiCache VM:</b> FCH-VM64, FCH-KVM	4.0, 4.1, 4.2

## FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
<b>FortiDDoS:</b> FI-1500E, FI-2000E	5.0
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.4
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.2
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.0
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E <b>FortiMail Low Encryption:</b> FE-3000C-LENC	5.4
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B <b>FortiMail Low Encryption:</b> FE-3000C-LENC <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3

## FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-2000E, FPX-4000E <b>FortiProxy VM:</b> FPX-KVM, FPX-VM64	1.0, 1.1, 1.2

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000F, FSA-2000E, FSA-3000E, FSA-3000F <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	4.0
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	3.2
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	3.1
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-AWS, FSA-VM	3.0
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	2.5.2

Model	Firmware Version
<b>FortiSandbox VM:</b> FSA-KVM, FSA-VM	
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	2.4.1
<b>FortiSandbox VM:</b> FSA-VM	2.3.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D	2.2.0
<b>FortiSandbox VM:</b> FSA-VM	

## FortiSOAR models

Model	Firmware Version
<b>FortiSOAR VM:</b> FSR-VM	6.4
<b>FortiSOAR VM:</b> FSR-VM	6.0

## FortiSwitch ATCA models

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	5.0.0
<b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3.0
	4.2.0

## FortiTester models

Model	Firmware Version
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E	3.9
<b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL	
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E	3.8
<b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL	
<b>FortiTester:</b> FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E	3.7
<b>FortiTester VM:</b> FortiTester-VM, FortiTester-VM-ALI-BYOL	

## FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.2, 6.3
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVEN	6.0
<b>FortiWeb:</b> FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6

Model	Firmware Version
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E	5.5
<b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E	5.4
<b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	



# Compatibility with FortiOS Versions

This section highlights compatibility issues that administrators should be aware of in FortiManager 6.4.7.

## FortiManager 6.4.7 and FortiOS 6.4.9 compatibility issues

This section identifies interoperability issues that have been identified with FortiManager 6.4.7 and FortiOS 6.4.9 in mantis 765709. FortiOS 6.4.9 includes syntax changes not supported by FortiManager 6.4.7.

The following default values changed:

- system snmp community events **default value changed from** cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-change bgp-established bgp-backward-transition ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-oversize-passed av-oversize-blocked ips-pkg-update ips-fail-open faz-disconnect wc-ap-up wc-ap-down fswctl-session-up fswctl-session-down load-balance-real-server-down per-cpu-high dhcp **to** cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-change bgp-established bgp-backward-transition ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-oversize-passed av-oversize-blocked ips-pkg-update ips-fail-open faz-disconnect wc-ap-up wc-ap-down fswctl-session-up fswctl-session-down load-balance-real-server-down per-cpu-high dhcp pool-usage.
- system snmp user events **default value changed from** cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-change bgp-established bgp-backward-transition ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-oversize-passed av-oversize-blocked ips-pkg-update ips-fail-open faz-disconnect wc-ap-up wc-ap-down fswctl-session-up fswctl-session-down load-balance-real-server-down per-cpu-high dhcp **to** cpu-high mem-low log-full intf-ip vpn-tun-up vpn-tun-down ha-switch ha-hb-failure ips-signature ips-anomaly av-virus av-oversize av-pattern av-fragmented fm-if-change bgp-established bgp-backward-transition ha-member-up ha-member-down ent-conf-change av-conserve av-bypass av-oversize-passed av-oversize-blocked ips-pkg-update ips-fail-open faz-disconnect wc-ap-up wc-ap-down fswctl-session-up fswctl-session-down load-balance-real-server-down per-cpu-high dhcp pool-usage.

The following objects were added:

```
(attr) system automation-action verify-host-cert
(attr) system global early-tcp-npu-session
(attr) system ha uninterruptible-primary-wait
(attr) system interface dhcp-relay-request-all-server
(attr) system netflow interface
(attr) system netflow interface-select-method
(attr) system sdn-connector verify-certificate
(attr) system sflow interface
```

```
(attr) system sflow interface-select-method
(attr) system vdom-netflow interface
(attr) system vdom-netflow interface-select-method
(attr) system vdom-sflow interface
(attr) system vdom-sflow interface-select-method
(attr) vpn ipsec phase1 inbound-dscp-copy
(attr) vpn ipsec phase1-interface inbound-dscp-copy
(attr) vpn ipsec phase2 inbound-dscp-copy
(attr) vpn ipsec phase2-interface inbound-dscp-copy
(attr) vpn ssl settings ciphersuite
(attr) vpn ssl settings status
(attr) wireless-controller apcfg-profile ap-family
```

### Additional option changes:

```
router multicast6 interface
    tag: tz -> None
system snmp community events
    option-list (tag|opt): None -> ["pool-usage"]
system snmp user events
    option-list (tag|opt): None -> ["pool-usage"]
system vdom-link type
    option-list (tag|opt): None -> ["npupair"]
system vxlan
    tag: nat -> None
vpn ssl settings banned-cipher
    option-list (tag|opt): None -> ["AESCCM", "ARIA", "CHACHA20"]
```

# Resolved Issues

The following issues have been fixed in 6.4.7. To inquire about a particular bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
633171	There may be <i>DFS Channel</i> mismatch between FortiManager and FortiGate for FAP-223E.
677419	FortiManager may show installation error on dual-5G radio band while pushing <code>wireless-controller</code> configuration.
682443	FortiManager should allow setting the index floor value and AP location should not be lost.
689325	FortiManager may not be able to configure <i>Channel 13</i> for Germany AP profile.
698004	When installing to a 6.4 FortiGate device from a 6.2 ADOM, there may be issue with <code>set vap-all manual</code> within the AP Profile.
702114	FortiManager is unable to see <i>5Ghz Clients</i> in <i>Health Monitor</i> .
716135	There may be verification error when trying to install FortiAP with 2.4GHZ <i>Radio 1</i> channel disabled.

## Device Manager

Bug ID	Description
563690	Device Manager fails to add FortiAnalyzer which contains a FortiGate HA device with error: <i>serial number does not match database</i> .
615044	Configuration status may be shown as <i>modified</i> after adding FortiGate to FortiManager.
640907	FortiManager is unable to configure FortiSwitch port mirroring.
665207	FortiManager needs IPv6 support on <i>Syslog</i> server setting.
670577	When creating an API admin from CLI Configuration, the <i>trusted host</i> section is missing.
674123	<i>SD-WAN template &gt; SD-WAN Rules</i> options for <i>Load Balance Mode</i> do not match that on FortiOS.
690493	<i>License check</i> setting may not be saved.
692200	FortiManager may return conflict after a <code>zero-touch-provisioning</code> cluster deployment.

Bug ID	Description
696730	FortiManager is unable to promote <i>Secondary</i> FortiGate as <i>Primary</i> in a HA Cluster.
697148	Interfaces that are members of SD-WAN and with interface-based traffic shaping applied should be displayed in the <i>Traffic Shaping</i> widget.
697596	<i>Advanced Options</i> is not displayed when creating a new interface.
702906	<i>DHCP Relay Service</i> may not be deleted when it is configured on VLAN interface.
705448	Device connection status may remain <i>Up</i> after shutting down device port and update device status.
709214	<i>System</i> template should allow <i>Source Interface</i> to be selected when <i>specify</i> is activated as <i>interface-select-method</i> .
711005	Under backup ADOM, FortiManager should hide the selection for <i>Provisioning Templates</i> and <i>Policy Packages</i> in the <i>Add Device</i> wizard, device <i>Dashboard</i> , and device <i>Edit</i> page.
711713	<i>DHCP relay</i> is displayed as <i>DHCP server</i> when Workspace is unlocked.
711888	FortiManager is not retrieving and saving the <code>vdom-exception</code> configuration.
714036	SD-WAN widget cannot be loaded when a rule uses a specific SLA target.
714208	<i>Device Manager</i> may not be able to save <code>scan-botnet-connections</code> option in interface settings page.
714611	Creating interface from VDOM may return <i>No Match Found</i> error.
714710	Secondary interface configuration may not show on <i>Device Manager</i> .
718184	AutoUpdate with <code>unset options &amp; unset post-lang</code> may cause device database and policy package status to show <i>OUT-OF-SYNC</i> .
719028	FortiManager may not update FortiGate's VDOM license information when it is changed.
719968	<i>SD-WAN Monitor</i> should show the proper <i>Map View</i> of all devices.
726359	After upgrade, Device Manager may not show managed devices after switching from <i>Table View</i> to <i>Map View</i> .
726990	When an administrator has access to a specified device group, FortiManager may remove devices that do not belong to the group when synchronizing device list to FortiAnalyzer.
728655	Configuration status may not be shown as <i>Synchronized</i> after installation.
728687	Policy package status may change to <i>Modified</i> on all FortiGate devices when a dynamic address group changes.
729301	A managed FortiGate with assigned CLI template remains in <i>modified</i> state following a successful device configure installation.
731551	FortiManager may return error, <i>Failed to synchronize FortiAnalyzer with current ADOM data.Fail(errno=-3):Object does not exist</i> , when adding FortiAnalyzer device.
733076	Model device links to real device may not work.

Bug ID	Description
733080	Device status appears in the GUI even though there is no activity for the session between FortiManager and FortiGate.
735106	<i>Delete</i> is spelled incorrectly when attempting to delete invalid host cluster device.

## FortiSwitch Manager

Bug ID	Description
700023	Install may fail with switch-controller managed-sweatshop-pre-standard-detection after upgrade.
716277	<i>FortiSwitch Manager</i> > <i>Managed Switches</i> tab is not in place after re-sorted.
740936	FortiSwitch VLAN template creates unknown interface platform mapping.

## Global ADOM

Bug ID	Description
667197	Users should not be able to delete global object when ADOM is not locked.
680798	FortiManager may return error, <i>Could not read zone validation results</i> , when assigning global ADOM changes with <i>Automatically Install Policies to ADOM Devices</i> .
693510	<i>Display Options</i> for <i>Object Config</i> will reset to default after sometime.
710963	FortiManager may show unclear error message when trying to promote an object from an ADOM to Global database under Workspace or Workflow mode.
722562	Users may not be able to filter ADOM when assigning Global Policy.
724229	Global ADOM display options may be reset to default after reboot.

## Others

Bug ID	Description
697361	FortiExtender status may not be correctly displayed.
724470	<code>dmworker</code> may crash on device retrieve or revision import.
728375	JSON API may return <code>"runtime error 0: invalid value"</code> error when getting dynamic mapping with <code>"fields"</code> attribute.

Bug ID	Description
732144	A CA certificate may be missing from some older FortiManager platforms causing failure to login with FortiCloud SSO.
679163	<i>Execute tac report</i> launched in CLI Widget fills the <i>/tmp</i> and prevents retrieval of FortiGate's configuration.

## Policy and Objects

Bug ID	Description
487186	FortiManager may install a different local category ID to FortiGate causing conflict with custom URL rating list.
569446	Interface subnet address object may show <i>any</i> as interface instead of the selected interface.
636537	<i>CLI Only Objects &gt; User &gt; peergrp</i> is not able to delete <i>peergrp</i> .
642708	<i>View Mode</i> may unexpectedly change from <i>Interface Pair View</i> to <i>By Sequence</i> mode.
654172	There may be webfilter local category ID mismatch between FortiManager and FortiGate causing incorrect action when using Custom URL List.
663109	FortiManager should not allow user to select a profile group in a flow-based policy that uses a proxy-based feature.
666091	After cloning a policy package, the cloned policy package loses the installation targets.
666258	User should not be able to create a firewall policy with an <i>Internet service</i> with <i>Destination direction in Source</i> by using drag and drop.
677528	<i>Address object</i> search may not display the address group which contains the searched object within the group.
679282	Editing a global object in an ADOM is not possible and generates the error, " <i>undefined is not iterable</i> ".
686911	Workflow session may not be able to compare with error: " <i>Can not compare because of invalid Revision Diff data</i> ".
690231	<i>Where-used</i> may fail to display references to <i>certificate-inspection</i> that were added to firewall policies in previous versions.
690295	FortiManager may be slow when multiple users access GUI at the same time.
696489	URL Filter under <i>Web Filter</i> profile may not be enabled properly.
701526	There may be issue to scroll down to view policy consistency results.
704148	FortiManager is missing some IPS signatures while they are available on FortiGate.
704637	FortiManager allows VIP to be configured without default value or dynamic mapping.
705189	" <i>config authentication scheme</i> " policy is not available for more than one FortiGate on the

Bug ID	Description
	same policy package.
712213	Users may not be able to filter policy using <i>Inspection Mode</i> field.
715269	<i>CVE-2021-26857</i> default action should be <i>Drop on the FortiManager</i> when the IPS version is greater than 18.028.
715275	FortiManager may not be able to show a specific signature.
715722	Users may not be able to delete a Global Object.
716114	FortiManager should push changed in ssl-ssh-profile with <i>Untrusted SSL Certificates</i> setting reverted from <i>Block</i> to <i>Allow</i> .
719698	Performance for policy install may be slightly degraded after upgrading from 6.4.5 to 6.4.6.
719700	FortiManager may have incorrect IPS default action entries in database.
719981	<i>Where Used</i> function may return no result for <i>Internet Service</i> objects.
720896	SSO admin with a <i>Restricted Admin</i> profile should be able to view <i>Web Filter</i> , <i>Application Control</i> , or <i>IPS</i> objects.
722087	Edit user group with remote members on FortiManager GUI may cause unexpected change in <i>set group-name</i> .
723409	After upgrade, installing to policy to FortiOS 6.0 devices may fail.
724718	When FortiManager's NSX-T connector is executing an API request, it should not be limited to 50 records.
725132	When modifying the IP address of <i>Default VPN Interface</i> of spoke in <i>Device Manager</i> , the hub remote gateway should be modified to reflect that change.
725274	GUI may be slow when filtering many entries with DNS filter.
726424	IPS signature list may be empty after upgrade.
727329	FortiManager may fail to identify case sensitivity with an interface that has a similar name for the <i>Normalized Interface</i> settings.
729287	User may not be able to edit DNAT.
730487	Copy procedure may stall at 67% with <code>securityconsole</code> crashes when copying policy package.
730523	Unused policies tool may always generate a PDF containing all policies.
732208	The <code>ip_addresses</code> from NSX-T are incorrectly <i>Resolved To</i> in FortiManager.
738109	FortiManager may not install auth-cert from policy package to device.
738745	When an object is renamed, the new name must be used on all policies.
738595	FortiManager may not correctly push AWS connector credentials.

## Revision History

Bug ID	Description
642878	FortiManager should return a clear copy fail log for dynamic interface check error.
683728	Installation fails due to VIP mapped IP range error when installing v6.2 policy package to v6.4 device.
691240	FortiManager should not unset the value of <code>forward-error-correction</code> with certain FortiGate platforms.
708913	FortiManager may try to set <code>sflow-counter-interval</code> and unset trunk-member resulting in installation failure.
711314	VDOM specific <i>Disclaimer Page</i> configuration is purged from <i>default</i> <code>replacemsg-group</code> during Policy Package installation.
724340	FortiManager may unset <code>forward-error-correction</code> from FortiGate 7060E devices.
724976	In <i>Zero Touch Provisioning</i> deployment, device database may get wiped by an <i>AutoRetrieve</i> task.
725717	After upgrade, installation may fail due to <code>mcast-session-counting</code> .
728117	After upgrade, install may fail due to <code>set pri-type-max 1000000</code> .
728422	Policy validation may fail due to dynamic mapping for global object that is for FortiGate 6.2 device but it is in 6.0 ADOM.
733518	FortiManager may incorrectly move DNAT objects.
735988	<i>Switch</i> and <i>AP</i> names may be reverted by controller status update from FortiGate.
742242	Install fails after upgrade due to <code>set server-identity-check enable</code> on LDAP server configuration.

## Script

Bug ID	Description
630016	FortiGate users can see scripts from all ADOMs.
689775	Users may not be able to edit an empty <i>CLI Script Group</i> .
707952	Copying of <i>CLI Script Group</i> from one ADOM to another ADOM may not work.
715632	Script configuring AntiVirus quarantine may fail.
721740	FortiManager may fail to run CLI script on Device DB after <code>dmworker</code> crash.
729571	TCL script commands run on device no longer show in the script log.



## Services

Bug ID	Description
567664	HA secondary device does not update FortiMeter license.
673302	FDS updates may fail with TLS v1.3.
685678	When FortiMail <i>FIPS</i> mode is enabled, FortiManager should be able to validate its license.
688498	FortiSwitch version shown in the FortiGuard package page is not seen on FortiGate.
700579	FortiManager should be able to provide the license information for isolated FortiSanbox.
702001	When receiving valid FCP updates, FortiManager should remove <i>mode/</i> flag for non FortiGate platforms.
704057	FOS-VM may not be able to update ISDB due to no contract on FortiManager.
725721	FortiManager may not be able to recognize all FortiGate units within an HA cluster, and it may not be able to update services to all units.
733174	FortiManager may not be able to recognize the object id 06002000NIDS02604as <i>IPS Signature Database(Extended)</i> .

## System Settings

Bug ID	Description
663185	<i>Search</i> may not work for event logs in text mode.
672954	Users should not be able to disable ADOM when there is non-root ADOM.
687968	FortiManager should not change to <code>ipv6-autoconf</code> to disable when management access is changed to the <code>ipv6-autoconf</code> enable state.
700608	The variable from meta data that is shown as not case sensitive, whereas the variable is case sensitive when using in a CLI template.
705145	Username is truncated to 49 characters in the notification Emails sent by FortiManager for workflow approvals.
709873	Global task assignment time may not be accurate.
711686	Workflow approval does not work when admin name has more than 49 characters.
722320	The <i>NOT</i> search in advanced/text mode search is not working for system event logs.
723117	Admin user may not be able to see who has locked an ADOM.
726007	Admin User systematically gets access to <i>Root</i> ADOM in case of RADIUS authentication and "Fortinet-Vdom-Name" VSA not set.
726138	After upgrade, FortiSwitch Template setting 'poe-pre-standard-detection' may cause

Bug ID	Description
	installation failure.
727458	FortiManager may not allow users to access all the VDOMs within an ADOM.
738395	FortiManager tasks' time used should not be increased by timezone.

## VPN Manager

Bug ID	Description
712861	<i>Policy Package Status</i> stays Synchronized despite SSL-VPN Portal configuration is changed using VPN Manager.

# Known Issues

The following issues have been identified in 6.4.7. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
733934	During zero-touch-provisioning with <i>Enforce Firmware Version</i> enabled, upgrade task may hang if the connection is reset during the image transfer.
740893	Secondary IP may be purged when setting a description to VLAN interface.

## Others

Bug ID	Description
657997	Assigning device to system template may not work via JSON when FortiManager is in Workspace mode.

## Policy & Objects

Bug ID	Description
585177	FortiManager is unable to create VIPv6 virtual server objects.
720673	Many groups learned from Cisco ISE may be missing corresponding ADOM objects.
726105	CLI-Only objects may not be able to select FSSO interface.
729179	FortiManager may not be able to add Geography type address when interface mapping is enabled.
765709	FOS 6.4.9 syntax support. See <a href="#">FortiManager 6.4.7 and FortiOS 6.4.9 compatibility issues on page 33</a> .

## Revision History

Bug ID	Description
741543	Install may fail with unset MAC address on EMAC VLAN.
496870	Fabric SDN connector is installed on FortiGate, even if it is not in use.

## Script

Bug ID	Description
384139	Filter does not work on device group.
654700	Users need to open <i>View Script Execution History</i> to see that TCL script fails.

## Services

Bug ID	Description
725118	FortiManager may not log FortiGuard connectivity failures.

## System Settings

Bug ID	Description
579964	FMG-VM64-Cloud needs to provide GUI support for ADOM upgrade in system information dashboard.
640670	If a user specified ADOM includes a global ADOM, workflow approval may not be able to find the same user.
721153	Scroll bar is missing from device drop-down list on ADOM overview page.
729280	Admin User with no access to management ADOM or VDOM can create a new VDOM from non-management ADOM > VDOM.
738622	ADOM upgrade from 6.0 to 6.2 may fail due to FortiExtender object.

## Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

### FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			



To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
set status enable
end
```

## Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

### Hardware models

The following table identifies the default number of ADOMs supported for FortiManager hardware models G series and later. It also identifies the hardware models that support the ADOM subscription license and the maximum number of ADOMs supported.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
3000G Series	4000	✓	8000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the [FortiManager Data Sheet](#).

### Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the [FortiManager Data Sheet](#).



**FORTINET®**



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.